

日 本 国 特 許 庁
PATENT OFFICE
JAPANESE GOVERNMENT

Jc714 U.S. PTO
09/654436
09/01/00

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日
Date of Application:

1999年 9月 1日

出 願 番 号
Application Number:

平成11年特許願第247994号

出 願 人
Applicant (s):

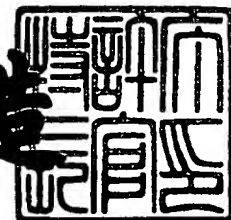
日本電信電話株式会社

CERTIFIED COPY OF
PRIORITY DOCUMENT

2000年 8月 4日

特許庁長官
Commissioner,
Patent Office

及 川 耕 造



出証番号 出証特2000-3060891

#2
Jc714 U.S. PTO
09/654436
09/01/00

PATENT OFFICE
JAPANESE GOVERNMENT

This is to certify that the annexed is a true copy of the following application as filed with this Office.

Date of Application: September 1, 1999
Application Number : P11-247994
Applicant(s) : Nippon Telegraph & Telephone Corporation

August 4, 2000

Commissioner,
Patent Office Kouzou OIKAWA

Number of Certificate: H 2000-3060891

【書類名】 特許願

【整理番号】 NTTH115898

【提出日】 平成11年 9月 1日

【あて先】 特許庁長官殿

【国際特許分類】 H04L 9/28
G06F 13/00

【発明の名称】 分散時刻認証装置および方法と分散時刻認証プログラム
を記録した記録媒体

【請求項の数】 4

【発明者】

 【住所又は居所】 東京都千代田区大手町二丁目 3 番 1 号 日本電信電話株式
 会社内

 【氏名】 田倉 昭

【発明者】

 【住所又は居所】 東京都千代田区大手町二丁目 3 番 1 号 日本電信電話株式
 会社内

 【氏名】 小野 諭

【特許出願人】

 【識別番号】 000004226

 【氏名又は名称】 日本電信電話株式会社

 【代表者】 宮津 純一郎

【代理人】

 【識別番号】 100083806

 【弁理士】

 【氏名又は名称】 三好 秀和

 【電話番号】 03-3504-3075

【選任した代理人】

 【識別番号】 100068342

 【弁理士】

【氏名又は名称】 三好 保男

【手数料の表示】

【予納台帳番号】 001982

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9701396

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 分散時刻認証装置および方法と分散時刻認証プログラムを記録した記録媒体

【特許請求の範囲】

【請求項 1】 入力されるデジタル文書に複数の時刻情報を結合して時刻印付きデジタル文書を作成する複数の結合手段と、

この結合手段から出力される時刻印付きデジタル文書に対しデジタル署名を作成する複数のデジタル署名手段と、

これら複数のデジタル署名手段からそれぞれ出力される複数のデジタル署名を受け取り、該デジタル署名の中から互いに等しい時刻情報の時刻印付きデジタル文書から作成されたデジタル署名を選択し、これら選択されたデジタル署名から統合デジタル署名を作成する統合デジタル署名作成手段と、

前記時刻印付きデジタル文書および統合デジタル署名とを含む時刻認証証明書を作成する時刻認証証明書作成手段と

を有することを特徴とする分散時刻認証装置。

【請求項 2】 前記結合手段に対し外部から送られたデジタル文書を受け取る文書受取手段と、前記時刻認証証明書作成手段により作成された時刻認証証明書を前記デジタル文書の送り元に送付する送付手段を有することを特徴とする請求項 1 記載の分散時刻認証装置。

【請求項 3】 入力されるデジタル文書に複数の時刻情報を結合して複数の時刻印付きデジタル文書を作成する手順と、

作成された複数の時刻印付きデジタル文書に対しそれぞれデジタル署名を作成する手順と、

これら複数のデジタル署名を受け取り、該デジタル署名の中から互いに等しい時刻情報の時刻印付きデジタル文書から作成されたデジタル署名を選択し、これら選択されたデジタル署名から統合デジタル署名を作成する手順と、

前記時刻印付きデジタル文書および統合デジタル署名とを含む時刻認証証明書を作成する手順と

を有することを特徴とする分散時刻認証方法。

【請求項 4】 入力されるデジタル文書に複数の時刻情報を結合して複数の時刻印付きデジタル文書を作成する手順と、

作成された複数の時刻印付きデジタル文書に対しそれぞれデジタル署名を作成する手順と、

これら複数のデジタル署名を受け取り、該デジタル署名の中から互いに等しい時刻情報の時刻印付きデジタル文書から作成されたデジタル署名を選択し、これら選択されたデジタル署名から統合デジタル署名を作成する手順と、

前記時刻印付きデジタル文書および統合デジタル署名とを含む時刻認証証明書を作成する手順と

をコンピュータに実行させる分散時刻認証プログラムを記録した記録媒体。

【発明の詳細な説明】

【0 0 0 1】

【発明の属する技術分野】

本発明はデジタル文書に時刻印を押すサービスにおいて、デジタル文書が時刻印を押された時点以降において変更されてなく、かつ確かに時刻印が押された時点で対象とするデジタル文書が存在していたことを証明することを可能とする時刻認証装置に関し、さらに詳しくは公開鍵暗号方式における分散署名を複数の分散時刻認証機関が独立して行い、分散時刻認証機関で作成された部分時刻署名から一つの結合時刻署名を得てから、元のデジタル文書の時刻認証証明書を得る方式に関し、集中型の時刻署名における秘密鍵に対する盗難などの危険性を排除することが可能な分散時刻認証装置および方法と分散時刻認証プログラムを記録した記録媒体に関する。

【0 0 0 2】

【従来の技術】

従来、デジタル文書に時刻印を押すサービスとして、特開平 7－2 5 4 8 9 7 号公報に記載の「個人用日時認証装置」が知られる、この個人用日時認証装置は、スマートカード等に時刻認証装置を組み込み、デジタル署名を行うときに時刻認証と一緒に行うものである。また、特開平 3－1 8 5 5 5 1 号公報に記載の「デジタル時間認証装置」は、時刻認証装置を一つのハードウェアプラットフォーム

として作成し、文書の作成者がその装置を使って時刻認証を行うものである。これらはいずれも、文書作成者が時刻認証を行う方式であるため、偽造がしやすく、第三者機関による証明でないため信頼性が乏しいものとなっている。

【 0 0 0 3 】

また特開平 6 - 1 4 0 1 8 号公報に記載の「電子的公証方法および装置」は、元の文書に対する CRC (Cyclic Redundancy Check ; 巡回冗長検査)、パリティ、検査合計を組み合わせて圧縮文書を作成し、時刻認証を行うものである。この方式で作成される圧縮文書は、現在広く暗号技術として使われているハッシュ関数（例えば MD 5 や SHA - 1 など）を用いて作成する圧縮文書と比較して同一の圧縮文書をもつデジタル文書の偽造がしやすい。

【 0 0 0 4 】

さらに特表平 6 - 5 0 1 5 7 1 号公報に記載の「数値文書に確実にタイムスタンプを押す方法」は、時刻認証を行う外部機関が単独で時刻認証証明書を作成するものである。このタイムスタンプを押す方法は、外部機関が時刻認証証明書を偽造することが容易である。

【 0 0 0 5 】

この欠点を補うために、受け取った時刻認証要求とその外部機関が直前に発行した時刻認証証明書を結合したデジタル文書に対してハッシュ関数を適用して得られた圧縮文書にデジタル署名を行い時刻認証証明書を作成する方法が提案されている。この方法は、時刻認証外部機関が時刻認証証明書を偽造することを事実上不可能にしている。

【 0 0 0 6 】

ところが、時刻認証証明書が真正であることを証明するためには、それ以前に発行した証明書のデジタル署名が必要となる。すなわち、時刻認証外部機関が発行したすべての時刻認証証明書を保存しておかないと、時刻認証証明書が真正であることを証明することができない。このため、システムとして膨大な記憶容量が必要とされることになる。

【 0 0 0 7 】

現在、I E T F (Internet Engineering Task Force) においてハッシュ関数

により圧縮されたデジタル文書を外部機関に送付し、送付された圧縮デジタル文書に対して時刻認証証明書を作成するプロトコルの標準化が進められている。ここで標準化が検討されている方式においては、外部機関は1ヶ所で時刻認証証明書を作成するため、時刻認証証明書の偽造の可能性および時刻認証証明書を取得することが許されていない悪意のある第三者が不正に時刻認証証明書を取得する危険性を排除することができないという問題点をすでに含んでいる。

【0008】

【発明が解決しようとする課題】

また公開鍵暗号方式における分散署名を複数の分散時刻認証機関が独立して行う場合には、時刻認証を行う外部機関が一つの秘密鍵を用いてデジタル署名を行う場合における秘密鍵の盗難の危険性やデジタル文書の著作者と時刻認証外部機関が結託して過去にさかのぼった時刻印を押す偽造の危険性を排除するために、時刻認証装置の秘密鍵を複数のデジタル署名手段が分割して持ち、それぞれのデジタル署名手段が独立してデジタル署名を行うことを可能とする。

【0009】

これにより秘密鍵盗難の危険性を少なくするとともに、時刻を取得する手段とデジタル署名を行う手段を実行するすべての機関が結託しない限り時刻印を偽造することができないようにすることにより安全で信頼のおける時刻認証サービスを行う時刻認証外部機関を運営することができる。

【0010】

また、過去に発行した時刻認証証明書を一切保管する必要はなく、従来手法と比較して大幅に記憶容量を削減することが可能である。

【0011】

しかしながら、分散した時刻認証機関が部分秘密鍵を用いて同一のデジタル文書に時刻署名を独立に行う場合、全く同一の時刻を付けたデジタル文書にデジタル署名を行わないと、分散秘密鍵に対応する公開鍵でデジタル署名を検証することができない場合があった。

【0012】

本発明は、上記課題に鑑みてなされたもので、独立に時刻署名を分散して行う

ときの複数の部分デジタル署名結果から得られる統合デジタル署名を一つの公開鍵を用いて復号し得るようにする分散時刻認証装置および方法と分散時刻認証プログラムを記録した記録媒体を提供することを目的とする。

【0013】

【課題を解決するための手段】

前述した目的を達成するために、本発明のうちで請求項1記載の発明は、入力されるデジタル文書に複数の時刻情報を結合して時刻印付きデジタル文書を作成する複数の結合手段と、この結合手段から出力される時刻印付きデジタル文書に対しデジタル署名を作成する複数のデジタル署名手段と、これら複数のデジタル署名手段からそれぞれ出力される複数のデジタル署名を受け取り、該デジタル署名の中から互いに等しい時刻情報の時刻印付きデジタル文書から作成されたデジタル署名を選択し、これら選択されたデジタル署名から統合デジタル署名を作成する統合デジタル署名作成手段と、前記時刻印付きデジタル文書および統合デジタル署名とを含む時刻認証証明書を作成する時刻認証証明書作成手段とを有することを要旨とする。

【0014】

請求項1記載の本発明では、時刻認証を行うときに、各時刻取得手段が独立に取得した時刻を用いても、どの時刻取得手段においても少なくとも1つは共通する時刻を取得して、統合デジタル署名を作成できるようにするため、適切な幅のある刻みで時刻を取得し、かつ各時刻取得装置が複数回の時刻取得を行う。この結果、統合デジタル署名作成手段で、共通する時刻をもつ時刻印付きデジタル文書に対して行われるデジタル署名から統合デジタル署名を作成することが可能となる。

【0015】

また、請求項2記載の発明は、請求項1記載の結合手段に対し外部から送られたデジタル文書を受け取る文書受取手段と、同時刻認証証明書作成手段により作成された時刻認証証明書を前記デジタル文書の送り元に送付する送付手段とを有することを要旨とする。

【0016】

請求項 2 記載の本発明では、分散時刻認証装置をネットワーク上に配置し、通信を行って利用者からの時刻認証要求を受け付け、時刻認証証明書を通信用により利用者に返却する。これにより、ネットワークに接続されたパソコン上のデジタル文書に対する時刻認証証明書を通信用により使って取得することが可能となる。

【0017】

また、請求項 3 記載の発明は、入力されるデジタル文書に複数の時刻情報を結合して複数の時刻印付きデジタル文書を作成する手順と、作成された複数の時刻印付きデジタル文書に対しそれぞれデジタル署名を作成する手順と、これら複数のデジタル署名を受け取り、該デジタル署名の中から互いに等しい時刻情報の時刻印付きデジタル文書から作成されたデジタル署名を選択し、これら選択されたデジタル署名から統合デジタル署名を作成する手順と、前記時刻印付きデジタル文書および統合デジタル署名とを含む時刻認証証明書を作成する手順とを有することを要旨とする。

【0018】

さらに、請求項 4 記載の発明の分散時刻認証プログラムを記録した記録媒体は、入力されるデジタル文書に複数の時刻情報を結合して複数の時刻印付きデジタル文書を作成する手順と、作成された複数の時刻印付きデジタル文書に対しそれぞれデジタル署名を作成する手順と、これら複数のデジタル署名を受け取り、該デジタル署名の中から互いに等しい時刻情報の時刻印付きデジタル文書から作成されたデジタル署名を選択し、これら選択されたデジタル署名から統合デジタル署名を作成する手順と、前記時刻印付きデジタル文書および統合デジタル署名とを含む時刻認証証明書を作成する手順とをコンピュータに実行させる分散時刻認証プログラムを記録したことを要旨とする。

【0019】

請求項 4 記載の本発明にあっては、分散時刻認証プログラムを記録媒体として記録しているため、該記録媒体を利用して、その分散時刻認証プログラムの流通性を高めることができる。

【0020】

【発明の実施の形態】

以下、図面を用いて本発明の実施の形態について説明する。

【0021】

図1は本発明の一実施の形態に係る分散時刻認証装置1の構成を示すブロック図である。

【0022】

図1において、分散時刻認証装置1は、一定間隔をおいて少なくとも1回以上である n 回、各々独立にある一定の刻みの時刻情報 t_{i1}, \dots, t_{is} を取得する複数の時刻取得手段13a, 13b, \dots , 13sと、デジタル文書 M に時刻情報 t_{ij} を結合して、各々独立に時刻印付きデジタル文書 $M t_{ij}$ を作成する前記時刻取得手段13a, 13b, \dots , 13s毎に1つ存在する複数の結合手段11a, 11b, \dots , 11sと、該結合手段11a, 11b, \dots , 11s毎に1つ存在する各々独立にデジタル署名を作成する複数のデジタル署名手段15a, 15b, \dots , 15sと、該複数のデジタル署名手段15a, 15b, \dots , 15sで独立に作成された複数のデジタル署名を受け取り、該デジタル署名の中から互いに等しい時刻印付きデジタル時刻印付きデジタル文書 $M t$ から作成されたデジタル署名を各デジタル署名手段15a, 15b, \dots , 15s毎に1つ選択できるときに、それらの選択された互いに等しい時刻印付きデジタル文書 $M t$ に対して、作成されたデジタル署名から統合デジタル署名 c を作成する統合デジタル署名作成手段17と、前記時刻印付きデジタル文書 $M t$ および統合デジタル署名 c を含む時刻認証証明書 T を作成する時刻認証証明書作成手段19により構成される。

【0023】

以下、図1を参照して本実施の形態における分散時刻認証処理について説明する。ここでは結合手段11aの系を中心に説明を進めるが、他の系においても同様である。

【0024】

著作者により作成されたテキスト文書、画像情報、音声情報、バイナリ情報あるいはそれらの組み合わせからなるデジタル文書 M から、分散時刻認証装置1内の結合手段11aにおいて、時刻取得手段13aにより取得された時刻と結合さ

れ時刻印付きデジタル文書M t が作成される。この作成された時刻印付きデジタル文書M t に対するデジタル署名がデジタル署名手段 15 a により作成される。

【0025】

このように各デジタル署名手段 15 a, 15 b, ..., 15 s で作成されたデジタル署名は、統合デジタル署名作成手段 17 に集められる。

【0026】

さらに統合デジタル署名作成手段 17 は、共通の時刻を持つ時刻印付きデジタル文書M t がデジタル署名手段 15 毎に一つ選択することができるときには、それらの共通の時刻を持つ時刻印付きデジタル文書M t に対するデジタル署名から統合デジタル署名を作成する。続いて、時刻認証証明書作成手段 19 は、統合デジタル署名を作成するのに用いた時刻印付きデジタル文書M t と統合デジタル署名を含む時刻認証証明書Tを作成する。

【0027】

以下、デジタル署名作成について、一例をあげて説明する。なお、ここでは公開鍵暗号の具体例としてRSAを用いる。このRSA公開鍵暗号の説明は、辻井重雄、笠原正雄編著「暗号と情報セキュリティ」（昭晃堂）に詳しい。

【0028】

まず、p と q を十分大きな素数とし、

$$n = p q$$

とおく。そして、

$$\phi(n) = (p-1)(q-1)$$

と互いに素な整数 e を適当に定める。すなわち、

$$\gcd(e, (p-1)(q-1)) = 1$$

n と e を公開鍵とし、d を

$$ed = 1 \pmod{\phi(n)}$$

である整数とすると、p, q, d を秘密鍵とする。

【0029】

共通の時刻を持つ時刻印付きデジタル文書M t にハッシュ関数（例えばSHA-1 やMD5）を適用して得られるダイジェストを m とする。

【0 0 3 0】

さらに、

$$c = m^d \bmod n$$

とおく。このとき、 c を統合デジタル署名作成手段 1 7 により最終的に作成される統合デジタル署名とする。図 1 におけるデジタル署名手段 1 5 の総数を s とする。

【0 0 3 1】

このとき、 d を数の和で表現する。

【0 0 3 2】

$$d = d_1 + d_2 + \cdots d_s$$

とおく。

【0 0 3 3】

$$c_1 = m^{d_1} \bmod n, \cdots, \\ c_s = m^{d_s} \bmod n$$

とすると、 c_1, \cdots, c_s が s 個のデジタル署名手段 1 5 a, 1 5 b, \cdots , 1 5 s で作成されるデジタル署名となる。 (M, t, c) を含むデジタル文書が時刻認証証明書 T となる。

【0 0 3 4】

図 2 は、本発明に係る他の実施形態の基本構成を示すブロック図である。

【0 0 3 5】

図 2 において、分散時刻認証装置 3 は、デジタル文書 M を通信により受け取る文書受取手段 3 0 と、一定間隔をおいて少なくとも 1 回以上である n 回、各々独立にある一定の刻みの時刻情報 t_{i1}, \cdots, t_{is} を取得する複数の時刻取得手段 3 3 a, 3 3 b, \cdots , 3 3 s と、文書受取手段 3 0 で受けとったデジタル文書 M に時刻情報 t_{ij} を結合して、各々独立に時刻印付きデジタル文書 M, t_{ij} を作成する前記時刻取得手段 3 3 a, 3 3 b, \cdots , 3 3 s 毎に 1 つ存在する複数の結合手段 3 1 a, 3 1 b, \cdots , 3 1 s と、該結合手段 3 1 a, 3 1 b, \cdots , 3 1 s 毎に 1 つ存在する各々独立にデジタル署名を作成する複数のデジタル署名手段 3 5 a, 3 5 b, \cdots , 3 5 s と、該複数のデジタル署名手段 3 5 a

、35b、・・・、35sで独立に作成された複数のデジタル署名を受け取り、該デジタル署名の中から互いに等しい時刻印付きデジタル時刻印付きデジタル文書Mtから作成されたデジタル署名を各デジタル署名手段35a、35b、・・・、35s毎に1つ選択できるときに、それらの選択された互いに等しい時刻印付きデジタル文書Mtに対して、作成されたデジタル署名から統合デジタル署名cを作成する統合デジタル署名作成手段37と、前記時刻印付きデジタル文書Mtおよび統合デジタル署名cを含む時刻認証証明書Tを作成する時刻認証証明書作成手段39と、この時刻認証証明書作成手段39で作成された時刻認証証明書Tを通信によりデジタル文書の送付者に返送する送付手段41により構成される。

【0036】

図3及び図4は、本発明における取得時刻情報の関係を示す図である。図では、デジタル署名手段35が3つある場合を例に取得時刻情報の関係を示している。同図において、 t_{11} 、 t_{21} 、 t_{31} は、例えば3つの時刻取得手段33a、33b、33cが1回目に取得した時刻をそれぞれ表わし、 t_{12} 、 t_{22} 、 t_{32} は、3つの時刻取得手段33a、33b、33cが2回目に取得した時刻をそれぞれ表わす。また、 t_{i1} 、 t_{i2} 、 t_{i3} は3つの時刻取得手段が第1回目に時刻取得を行ったときの正確な時刻を表わす。

【0037】

図3では、3つの時刻取得手段33a、33b、33cとも1回目に同じ時刻情報を取得し、2回目も同じ時刻情報を取得したことを表わす。この場合には、 $t_{11}=t_{21}=t_{31}$ が統合デジタル署名の作成に用いられる時刻となる。同様に、図4では、 $t_{31}=t_{12}=t_{22}$ のみが統合デジタル署名の作成に用いられる時刻となる。

【0038】

このとき2回目以降の時刻取得を、実際には行わずに第1回目に取得した時刻に予め決められた刻み幅の時間を順次加えて得られた時刻を2回目以降の取得時刻とすることも可能である。

【0039】

通常、分散時刻認証装置にあっては、構成要素のデジタル署名手段が公開鍵暗

号における秘密鍵の一部を分散して保持するので、秘密鍵の盗難や時刻認証証明書の偽造の危険性を小さくすることができるものの、前述したように時刻取得手段が各々独立に取得した時刻が一致する可能性は非常に小さいため統合デジタル署名を作成できないという問題がある。

【 0 0 4 0 】

これに対し、本実施形態では上述してきたように、ある刻み幅で時刻を取得するので、各々独立に取得した時刻が等しくなる可能性が高い。さらに、一定間隔において最低 2 回の時刻取得を各時刻取得手段毎に行えば、刻み幅と一定間隔の取り方により必ず共通する時刻印付きデジタル文書をすべての結合手段で得ることが可能となる。この結果、秘密鍵の安全性を向上させる分散時刻署名が可能となる。

【 0 0 4 1 】

このような分散時刻認証プログラムは記録媒体に記録して提供されることにより当該分散時刻認証プログラムの流通性を高めることができる。

【 0 0 4 2 】

なお、上述した各実施の形態では、RSA を公開鍵暗号を用いて場合について説明したが、本発明はこれに限定されることなく楕円公開鍵暗号、DSA (Digital Signature Algorithm) 等の秘密鍵を分割し、単一の秘密鍵で作成するデジタル署名と同じデジタル署名を、複数の分割した秘密鍵から作成することが可能な公開鍵暗号を用いても同様にデジタル署名および統合デジタル署名を作成することが可能である。

【 0 0 4 3 】

また、時刻印付きデジタル文書 M_t の代わりに時刻印付きデジタル文書 M_t を含むデジタル文書を用いて統合デジタル署名を作成しても、何ら問題はない。さらにデジタル文書にハッシュ関数を適用せずに直接デジタル署名を作成することも可能である。また、1 つの時刻印付きデジタル文書 M_t に 1 つの時刻情報に対応させるものであっても、1 つの時刻印付きデジタル文書 M_t に複数の時刻情報に対応させるものであっても良い。つまり 1 つの時刻情報に対応する場合には 1 つの時刻印付きデジタル文書 M_t から 1 つのデジタル署名が作成され、複数の時

時刻情報に対応する場合には 1 つの時刻印付きデジタル文書 M t から複数のデジタル署名が作成されることになる。

【 0 0 4 4 】

【発明の効果】

以上、説明してきたように本発明の分散時刻認証装置によれば、必ず共通する時刻印付きデジタル文書をすべての結合手段で得ることが可能となるので、秘密鍵の安全性を向上させる分散時刻署名が可能となる。

【図面の簡単な説明】

【図 1】

本発明の基本構成を示すブロック図である。

【図 2】

本発明の他の実施形態における基本構成を示すブロック図である。

【図 3】

時刻取得方法と取得した時刻情報の用い方を説明する図である。

【図 4】

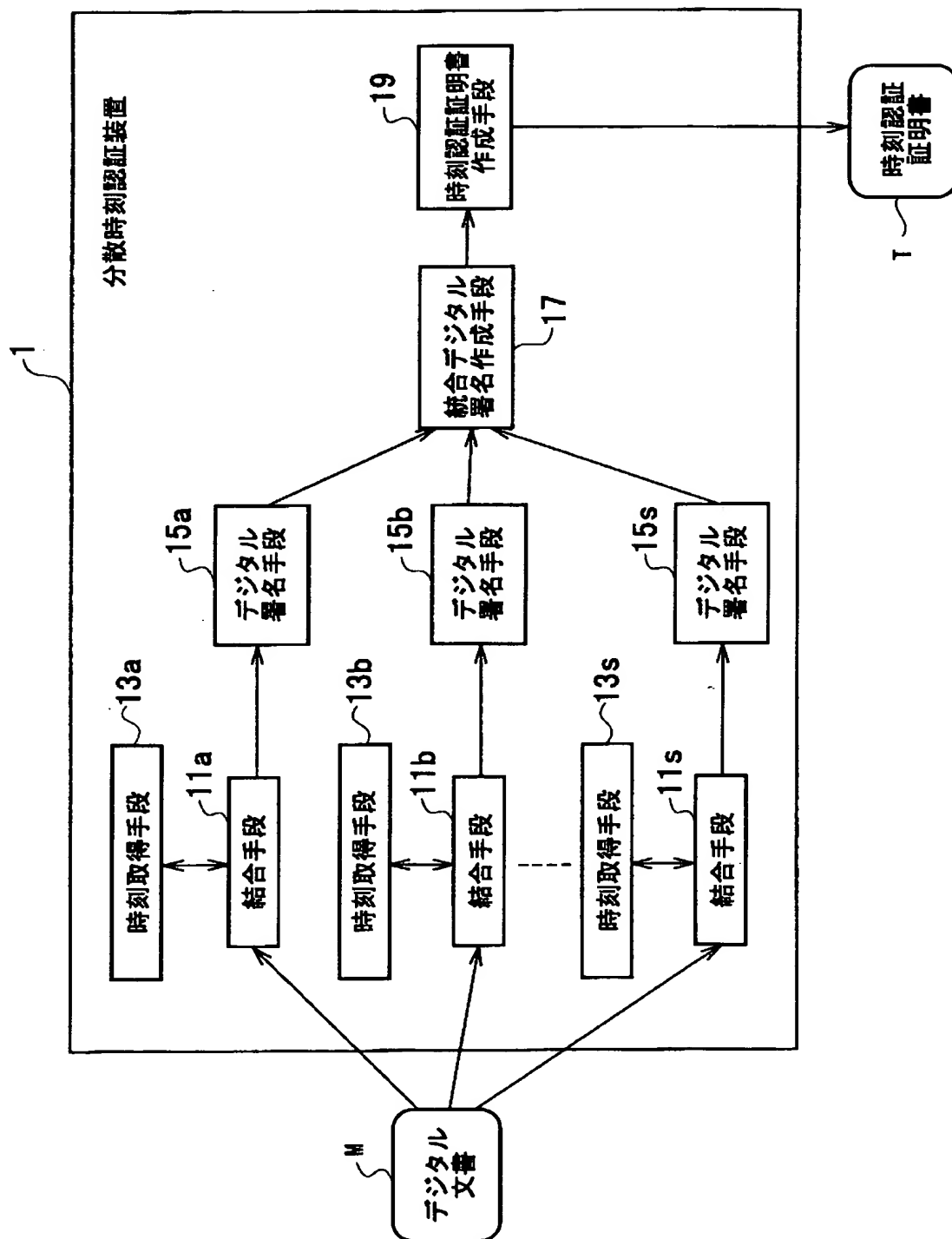
時刻取得方法と取得した時刻情報の用い方を説明する図である。

【符号の説明】

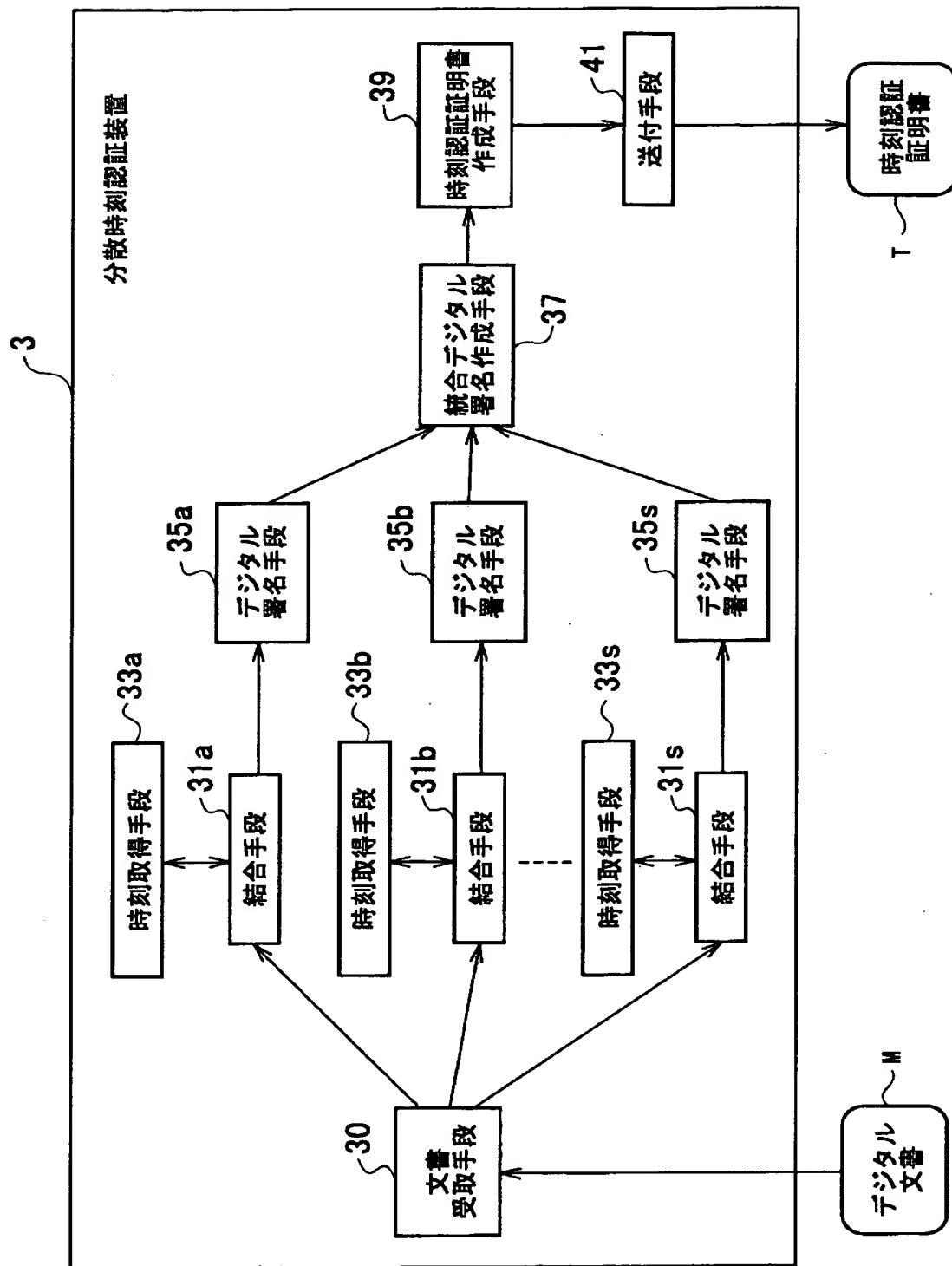
- 1, 3 分散時刻認証装置
- 1 1, 3 1 結合手段
- 1 3, 3 3 時刻取得手段
- 1 5, 3 5 デジタル署名手段
- 1 7, 3 7 統合デジタル署名作成手段
- 1 9, 3 9 時刻認証証明書作成手段
- 3 0 文書受取手段
- 4 1 時刻認証証明書の送付手段
- M デジタル文書
- T 時刻認証証明書

【書類名】 図面

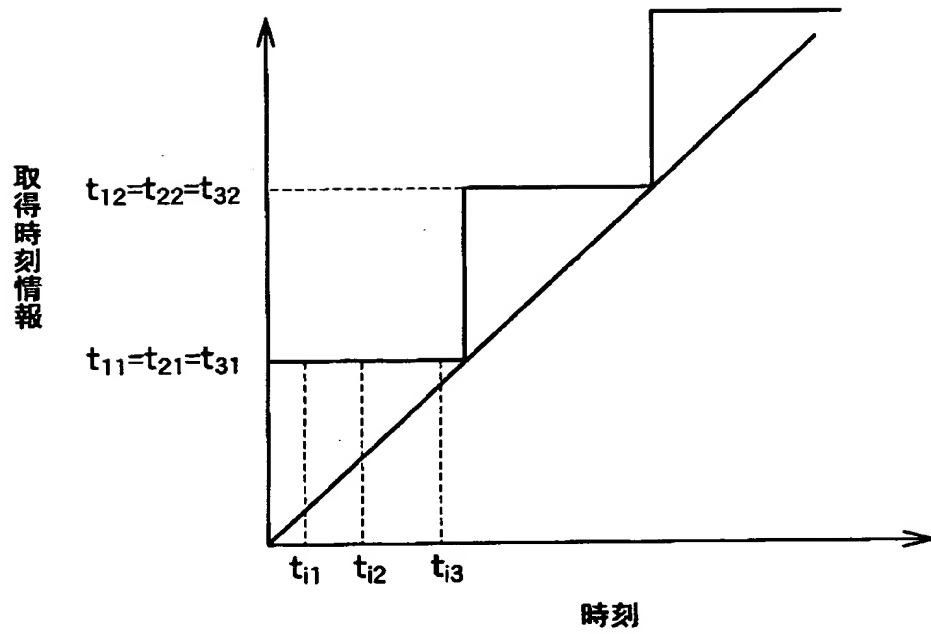
【図 1】



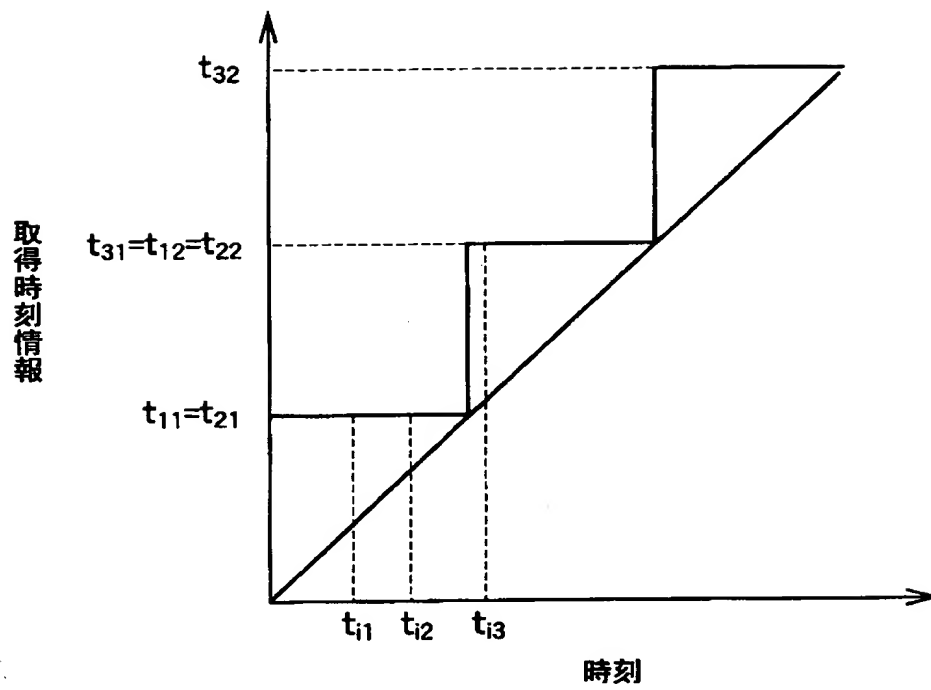
【図 2】



【図 3】



【図 4】



【書類名】 要約書

【要約】

【課題】 本発明は、独立に時刻署名を分散して行うときの複数の部分デジタル署名結果から得られる統合デジタル署名を一つの公開鍵を用いて復号し得るようにする分散時刻認証装置および方法と分散時刻認証プログラムを記録した記録媒体を提供することを目的とする。

【解決手段】 入力されるデジタル文書に複数の時刻情報を結合して時刻印付きデジタル文書を作成する複数の結合手段と、この時刻印付きデジタル文書に対しデジタル署名を作成する複数のデジタル署名手段と、これら複数のデジタル署名を受け取り、該デジタル署名の中から互いに等しい時刻情報の時刻印付きデジタル文書から作成されたデジタル署名を選択し、これら選択されたデジタル署名から統合デジタル署名を作成する統合デジタル署名作成手段と、前記時刻印付きデジタル文書および統合デジタル署名とを含む時刻認証証明書を作成する時刻認証証明書作成手段とを備えて構成される。

【選択図】 図 1

出 願 人 履 歴 情 報

識別番号 [000004226]

1. 変更年月日 1999年 7月15日

[変更理由] 住所変更

住 所 東京都千代田区大手町二丁目3番1号
氏 名 日本電信電話株式会社